

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

ContentGuard Holdings, Inc.,

Plaintiff,

v.

Amazon.com, Inc. *et. al*,

Defendants.

CIVIL ACTION NO. 2:13-cv-1112-JRG
Jury Trial Demanded

**DEFENDANTS' REPLY IN SUPPORT OF
RENEWED MOTION FOR JUDGMENT ON THE PLEADINGS DECLARING
ALL ASSERTED PATENT CLAIMS INVALID PURSUANT TO 35 U.S.C. § 101**

ContentGuard's Opposition does not address even a single complete claim from its eight asserted patents, nor does it even attempt to explain how the actual elements of any asserted claim, alone or in ordered combination, are directed to anything more than the age-old, abstract idea of enforcing usage rights and restrictions on content. Instead, ContentGuard's Opposition improperly lumps all of its twenty-six asserted patent claims together and broadly asserts *only* that the claims' reference to "trusted" devices somehow differentiates the claimed systems/methods from the *idea* of controlling content usage that has been practiced for centuries in lending libraries and, more recently, video rental stores. In essence, ContentGuard argues that because "trusted" devices (which the claims sometimes call "repositories") are programmed computers that possess three integrities—physical integrity (to prevent untrusted persons/software from accessing content), communications integrity (to prevent untrusted persons/software from "telling lies" to obtain content), and behavioral integrity (to assure that only known persons/software are permitted access to the system)—those "trusted" devices/"repositories" can enforce usage rights more reliably than humans, who are capable of error or dishonesty, such that the asserted claims are "technology-based." (Opp. at 8-12.)

Yet, simply substituting a reliable computer for a potentially unreliable person in a library loan or a video rental transaction does not entitle ContentGuard to a 20-year monopoly on the idea of enforcing usage rights on digital content (which libraries and video stores have been doing for CDs and DVDs for decades). The Supreme Court, this Court and virtually every other court having considered the issue have made crystal clear that simply using programmed computers to execute a known idea/method faster, more easily or more reliably cannot and will not make a claim patent-eligible. *See Alice Corp. Pty. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2357-58 (2014) (mere use of computer cannot render abstract idea patent eligible); *Clear with Computers LLC v. Altec Indus., Inc.*, No. 6:14-cv-79, Slip Op. at 7, 9 (E.D. Tex. Mar. 3, 2015) (invalidating claims that "invoke computer technology only to take advantage of the relative ease by which a computer, rather than a human salesman, could create individualized sales proposals to solve this problem"); *Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Canada*, 687 F.3d

1266, 1279 (Fed. Cir. 2012); *Loyalty Conversion Sys. Corp. v. Am. Airlines*, No. 13-655, 2014 WL 4364848, at *9, 10 (E.D. Tex. Sept. 3, 2014) (“speed and convenience” of computer implementation doesn’t make claim patentable); *Money Suite Co. v. 21st Century Ins. & Fin. Servs., Inc.*, No. 13-984, 2015 WL 436160, at *5 (D. Del. Jan. 27, 2015) (that a computer can “handle volumes and complexity at levels impossible for humans” is inherent in use of computers and does not render claim patentable); *Certusview Techs. LLC v. S&N Locating Servs.*, No. 13-346, 2015 WL 269427, at *20 (E.D. Va. Jan. 21, 2015) (use of technology to reduce effect of human error does not make abstract idea patentable).

Though ContentGuard attempts to distract the Court with legally irrelevant discussions of “these inventions’ background,” (Opp. at 2-4), “objective indicia on non-obviousness,” (*id.* at 16-17), and “the PTAB’s recent decisions” on matters *unrelated to Section 101*, (*id.* at 15-16), ContentGuard offers no legally sufficient explanation as to (a) how any of its asserted patent claims are directed to something other than the abstract idea of enforcing usage rights and restrictions on digital content, or (b) how any of its asserted patent claims involve “the type of complex programming that confers patent eligibility.” *Altec*, Slip Op. at 9. As the Court’s various claim constructions make clear, ContentGuard’s asserted claims require no specific computer hardware or software, and invoke only basic computer functions such as receiving and decrypting data, storing data, analyzing data and following instructions. Accordingly, like the claims invalidated by this Court in *Altec*, “[T]he instant claims and the *Ultramercial* claims fail for the same reason: they comprise only ‘conventional steps, specified at a high level of generality, which is insufficient to supply an inventive concept.’” *Id.* at 10 (quoting *Ultramercial v. Hulu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014), and *Alice*, 134 S. Ct. at 2357).

DISCUSSION

ContentGuard attempts to deflect a Section 101 analysis in two ways. First, a significant portion of the Opposition is devoted to extolling the alleged general novelty and importance of the patents collectively, *e.g.*, by explaining “the[] inventions’ background” (Opp. at 2-4), by discussing the “importance of DRM” generally, (*id.* at 5-6), by quoting articles on “library

technologies” from 10 years after the patents’ claimed priority date, (*id.* at 15), and by asserting “numerous ‘objective indicia of non-obviousness,’” (*id.* at 16-17). None of this is relevant. *Diamond v. Diehr*, 450 U.S. 175, 190 (1981) (§ 101 inquiry is distinct from other conditions of patentability); *In re TLI Comms. LLC Patent Litig.*, No. 14-2534, 2015 WL 627858, at *9 (E.D. Va. Feb. 6, 2015) (“plaintiff’s focus on novelty is misplaced; it conflates whether a patent is directed to eligible subject matter under § 101 with whether a patent meets § 102’s novelty requirement”); *Money Suite*, 2015 WL 436160, at *3 (argument that claim elements not in prior art “sound[s] in § 102 novelty [and] is beside the point for a § 101 inquiry”).

Second, ContentGuard avoids addressing *any* of the specific patent claims at issue, instead referring to each patent family—Stefik and Nguyen, and all of the asserted claims and elements therein—as one undifferentiated group. The Section 101 analysis, however, *requires an element-by-element analysis*, as Defendants performed in their motion. *Alice*, 134 S. Ct. at 2355 n.3, 2359. ContentGuard is thus woefully off the mark when it derogates Defendants for “spend[ing] 21 pages of their motion attempting to line up the myriad elements of the asserted claims with alleged ‘corresponding action[s]’ purportedly existing in bricks-and-mortar libraries,” (*Id.* at 8), especially after acknowledging that “in the context of a Section 101 analysis, it is not appropriate to ignore the claims’ *actual* limitations.” (Opp. at 7.)

ContentGuard’s conclusory characterization of the asserted claims as “technology-based inventions,” (Opp. at 1), and “pioneering”, (*id.* at 16), neither diminishes the impermissible breadth of the claims nor establishes how any claim elements, or their ordering, “transform the nature of the claim into a patent eligible application.” *Altec*, Slip Op. at 6 (quoting *Alice*, 134 S. Ct. at 2355, and *Mayo Collab. Servs. v. Prometheus Labs.*, 132 S. Ct. 1289, 1297-98 (2012)). ContentGuard’s naked urging that its patents teach “concrete, innovative solutions that address the challenge of protecting and distributing digital content in the advent of the Internet,” (Opp. at 7), cannot substitute for actual analysis of the Court’s claim constructions, of the specific claim elements, or of the scope of the asserted claims *as ContentGuard is attempting to apply those*

*claims in this litigation.*¹

I. The Stefik Patents

A. The Stefik Patents Are Drawn to Abstract Ideas.

Each Stefik patent claim is drawn to a computer implementation of the abstract idea of enforcing usage rights on digital content, as shown by Defendants’ hypotheticals. (Mot. at 7-28.) *See Content Extraction & Transmission v. Wells Fargo Bank, Nat’l Ass’n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (tying computer patent steps to analogous actions by humans shows claim drawn to abstract idea); *Altec*, Slip Op. at 7 (“The steps performed by the claimed computer elements are functional in nature and could easily be performed by a human.”). Stripped of its irrelevant discussions of obviousness and the inventions’ background, ContentGuard’s Opposition boils down to a single argument: the asserted claims purportedly are not directed to an abstract idea because they specify the use of “trusted” devices/“repositories” that have three integrities—physical, communications and behavioral. As stated by ContentGuard, “Of special significance here, however, is a particular aspect of Stefik’s innovations, specifically their teachings concerning ‘trusted’ systems. At bottom, Stefik’s vision was that ‘trusted systems . . . would be the only feasible way to implement digital rights management because general-purpose computers ha[d] too many security holes.” (Opp. at 3 (internal citations omitted).)

As carefully detailed in Defendants’ Motion, (Mot. at 10-14), however, analogues of the three “integrities”, as construed by the Court, are easily found in age-old library loan transactions. Physical integrity—“preventing access to information in its possession by a non-trusted person” (Dkt. 459 at 18)—is maintained (a) by locking a library’s doors at night and using security gates at entrances and exits to prevent people from walking out with library books and DVDs; (b) by a librarian’s authorization of a loan only to a patron who can show proof (in

¹ For example, the Court found that “usage rights” do not need to be statements in a specific computer-enforceable “language”, and that a “digital certificate” does not need to be issued by a third-party “master repository,” thus stripping out of the asserted claims limitations that *might* have imposed some restrictions on scope and application. Further, ContentGuard is now taking the position that any persistent “association” between a license and digital content—even licenses that are stored and transmitted separate from content, as in the *Griswold* art expressly distinguished by the Stefik patent specifications—can satisfy the requirement that usage rights be “attached, or treated as attached” to digital content. Thus, ContentGuard’s own infringement allegations in this case make very clear that the asserted reach of the Stefik patent claims is impermissibly wide and long.

the form of a valid library card) that she is trusted and authorized to borrow; and (c) by an authorized patron taking physical custody of borrowed materials and securely keeping them on her person and/or in her locked home.² Communications integrity—“only communicates with other devices that are able to present proof that they are trusted systems,” (Dkt. 459 at 18)—is maintained by a librarian only lending library materials to patrons who are able to present proof (in the form of a valid library card) that they are trusted and authorized borrowers. No library card, no ability to borrow. ContentGuard’s Opposition states with regard to communications integrity that, “A ‘library card’ is merely proof of the possessor’s identity; it is not a guarantee that he or she can safely receive valuable digital content and be *prevented* from misusing it once access is conveyed.” (Opp. at 9.) Yet the Court’s construction of communications integrity does not require a *guarantee* that a repository can safely receive content; it only requires that a receiving repository be able to present proof that it is “trusted”. A patron’s library card, which typically includes a picture of the patron and which only can be issued upon the patron’s commitment to abide by a library’s usage rules (often secured by a credit card number), certainly qualifies as “proof” that a patron is a trusted recipient.

Behavioral integrity—“requiring software to include a digital certificate in order to be installed in the repository,” (Dkt. 459 at 21)—is maintained by assuring that patrons and library employees possess appropriate “certificates” (a valid library card and a valid government-issued photo ID, respectively) before they are given access to the library’s materials. No valid certificate, no access to the “repository” or its materials. As noted in Defendants’ Motion (Mot. at 12), but ignored by ContentGuard, the Stefik patent specifications’ own description of “behavioral integrity” generally, and “digital certificates” specifically, establishes that this element involves merely conventional steps for verifying the source of software—steps already

² On the one hand, ContentGuard’s Opposition suggests that “Defendants point to nothing in the library setting that establishes the library patron’s ‘physical integrity’”, (Opp. at 8-9), and then, on the other hand, the Opposition labels Defendants’ recognition that a library patron takes personal possession of library materials, and maintains those materials in his physically secure bag and home, as “facially untenable.” (*Id.* at 9 n.5.) ContentGuard offers no explanation as to why or how a library patron’s physical possession and protection of library materials differs in any meaningful way from a computer’s maintenance of digital content in its secure memory. In both cases, untrusted persons are physically prevented from accessing content.

taken by human consumers: “The integrity of the software is generally assured only by knowledge of its source. Restated, a user will trust software purchased at a reputable computer store but not trust software obtained off a random (insecure) server on a network.” (Ex. 4 at 12:49-55 (emphasis added).)

ContentGuard urges the Court to find that these integrities as found in the traditional library lending transaction are “*not the same*” as the integrities exhibited by “trusted” devices/“repositories” of the Stefik patents. (Opp. at 8-9 (emphasis in original).) But beyond the fact that the integrities are maintained by humans and buildings in the library loan transaction and by computers and software in the Stefik patents’ usage rights transactions, ContentGuard can point to no meaningful difference between the integrities involved in the physical interaction between library/librarian and card-carrying patron and the digital interaction between a content-distributing computer and a content-receiving computer. The mere facts that (a) one interaction is digital rather than physical (and deals with “digital content” rather than printed books or videotapes), and (b) computers are more reliable in carrying out their instructions than are human librarians and patrons, makes no difference to the patentable subject-matter analysis. *See Alice*, 134 S. Ct. at 1357-58; *Loyalty*, 2014 WL 4364848, at *9, 10; *Money Suite*, 2015 WL 436160, at *5; *Certusview*, 2015 WL 269427, at *20.

Importantly, the Stefik patent specifications make very clear that the integrities/“security levels” for the referenced “trusted” systems/“repositories” are not fixed or specifically defined, and that the patent claims’ references to “trusted” systems/“repositories” are intended to capture only “the idea” of having security, not to define any specific, required security level: “The characterization of security levels described in Table 2 *is not intended to be fixed. More important is the idea of having different security levels for different repositories.* It is anticipated that new security classes and requirements will evolve according to social situations and changes in technology.” (Ex. 4 at 15:45-50 (emphasis added).) So, even Dr. Stefik acknowledged that “trusted” systems do not require any specific computer programming.

Moreover, ContentGuard’s Opposition does not dispute that the “technology-based

solution” purportedly suggested by the asserted claims utilizes only the most conventional and routine of computer actions and functions—secure storage, basic encryption/decryption and processing of data, and faithful execution of software instructions. Indeed, Defendants’ Motion points out, in great detail, how the Stefik specifications, themselves, recognize the prevalence in the prior art of the very techniques purportedly used by the patent claims to maintain the three integrities. (Mot. at 9-14). ContentGuard’s only response is to suggest that, “Even if true, this assertion is beside the point,” (Opp. at 14), because “the creation of new compositions and products based on combining elements from different sources has long been a basis for patentable inventions.” *Id.* (quoting *DDR Holdings, LLC v. Hotels.com L.P.*, 773 F.3d 1245 (Fed. Cir. 2014)). Yet ContentGuard fails to acknowledge that only combinations which add something concrete to the art, such as “inventive algorithms” or “complex programming”, *Altec*, Slip Op. at 9-10, can qualify as patentable subject matter: “‘A claim that recites an abstract idea must include additional features’ which ‘must be more than well-understood, routine, conventional activity.’” *Id.* at 8 (quoting *Ultramercial*, 772 F.3d at 715). Simply using basic computer functions to cause a computer to act as a digital librarian does not “provide an inventive concept sufficient to confer patent eligibility.” *Altec*, Slip Op. at 8.³

Just this month, the district court in *Jericho Systems Corp. v. Axiomatics, Inc.*, No. 3:14-CV-2281, Slip Op. (N.D. Tex. May 7, 2015) (attached hereto as Exhibit 17), invalidated patent claims extremely similar to ContentGuard’s on a motion for judgment on the pleadings pursuant to Section 101. Like ContentGuard’s claims, the patent claims at issue in *Jericho* disclosed “an invention used to make a decision regarding a particular person’s authority to access certain information. The invention does this by determining what type of information is needed to make

³ ContentGuard makes cursory and passing statements such as, “‘Prevent[ing] access to information by a non-trusted system,’ so as to implement ‘physical integrity,’ is no routine business activity, and Defendants have not proven otherwise.” (Opp. at 14.) But, such unsupported and unexplained statements by ContentGuard are wholly insufficient to establish patentability, particularly in light of the fact that Defendants *have* proven otherwise by explaining how in the library loan context, physical integrity is maintained (a) by locking a library’s doors at night and using security gates at entrances and exits to prevent people from walking out with library books and DVDs; (b) by a librarian’s authorization of a loan of library materials only to a patron who can show proof (in the form of a valid library card) that she is trusted and authorized to borrow; and (c) by an authorized patron’s taking physical custody of borrowed materials and securely keeping them on her person or in her locked home.

an access decision, obtaining that information, and then applying that information to a rule regarding access to the information. If the information satisfies the rule, then the person is allowed access. If not then the person is denied access.” *Id.* at 2.

The *Jericho* Court invalidated the claims despite their explicit reference to (a) “receiving, by a server, a rule associated with the [user] action, wherein the server comprises a processor and operatively associated memory, and wherein the rule indicates conditions under which a request to perform the action on the resource should be granted”, and (b) “evaluating, by the server, the user request to determine whether the user is authorized to perform the action on the resource, wherein the evaluation comprises applying the rule considering the values for the plurality of attributes.” *Id.* at 7. The court stated:

Claim 1 does not pass the first part of the *Mayo* two-part test because it recites an abstract idea. The wording of the claim appears to present a complex method that uses attributes, rules, connectors, classifications, and remote data sources. But, upon closer examination, the gist of the claim involves a user entering a request for access, looking up the rule for access, determining what information is needed to apply the rule, obtaining that information, and then applying the information to the rule to make a decision.

This is an abstract idea. The abstract idea being that people who meet certain requirements are allowed to do certain things. This is like [Defendant’s] example of making a determination if somebody is old enough to buy an R rated movie ticket. In order to make this determination, one would have 1) to determine the rule, which would be a person must be 17 to purchase an R rated movie ticket; 2) determine what information is needed to make a decision under the rule, which is the age of the person trying to buy a ticket; 3) retrieving the specific information about the person needed to make that determination, which is requesting proof of age; 4) applying that information to the rule, which may be yes the person is allowed to purchase the ticket because his age is 20.

Id. at 8-9. The *Jericho* Court rejected the patentee’s assertion (similar to ContentGuard’s present argument) that its claims were “rooted in computer technology.” The court explained:

The problem [of controlling access] existed before modern computing and the internet existed and the claimed invention simply uses standard computing and communication equipment and procedures to implement the abstract idea. This situation is much more like those presented in *Alice* and *Ultramercial*, in which computer technology was used to implement an idea, unrelated to the functioning of the computer or the Internet, in a faster and more efficient manner. In those cases and the case at hand, the mere fact that the process was faster and more efficient because it used computers is insufficient to convert an abstract idea into

a non-abstract idea or to root the invention in modern computer technology.

Id. at 11-12. There is little, if anything, to distinguish ContentGuard's claims from those invalidated in *Jericho*. The mere fact that ContentGuard's asserted patent claims mention the use of broadly defined "trusted" systems/"repositories", having three integrities that (a) find direct analogues in traditional library loan and video store transactions and (b) are implemented using "standard computing and communication equipment and procedures", (*id.* at 11), cannot and does not convert the abstract idea of enforcing usage rights on digital content into a non-abstract idea eligible for patenting. As with the claims invalidated in *Altec*, "There is no meaningful distinction for § 101 purposes between the abstract concept embodied by these claims and the abstract ideas identified in prior cases, and [Plaintiff] points to none." *Altec*, Slip Op. at 7 (*see also* myriad cases cited in footnote 3 to Defendants' Motion).

B. There is No Inventive Element in the Stefik Claims.

In an effort to suggest that its asserted claims teach "inventive concepts," ContentGuard first repeats its conclusory assertion that "the three integrities required to implement a 'trusted repository' are not merely the routine or conventional use of a general-purpose computer." (Opp. at 14.) However, as discussed above and in Defendants' Motion, (Mot. at 9-16), there is nothing about the three integrities that involves (let alone requires) the use of computer features that are "more than the well-understood, routine, conventional activity." *Altec*, Slip Op. at 8. Indeed, as construed by the Court, physical and communications integrity do not require *any* specific or defined hardware, algorithms or programming, (Dkt. 459 at 18); and behavioral integrity requires only that software include a conventional and routinely used "digital certificate" that attests to the source of the software, (*id.* at 21). These broadly defined integrities, alone or together, cannot constitute "inventive concepts" because

- (a) the patents themselves recognize that the computer elements, functions and techniques usable to maintain the integrities were "well-known" and conventionally used, (*see* Mot. at 9-16.) For example, the patents acknowledge that encryption and nonces, which can be used to establish both physical and communications integrity, were well-known and widely utilized in the art at the time of filing. *See, e.g.*, Ex. 4 at 26:2-4 ("Public key encryption is a

well-known technique in the encryption arts.”); *id.* at 3:31-35 (explaining that in the prior art Sprague patent, “A plurality of encrypted information packages (IPs) are provided at the user site, The IPs of interest are selected by the user and are decrypted and stored locally.”); *id.* at 27:43-48 (describing known use of nonces). And the patents recognize that prior to the patent applications, multiple systems possessing the three integrities were available, and were being used, for enforcing usage rights on digital content. *See, e.g.*, Ex. 4 at 1:65-2:4 (“For existing materials that are distributed in digital form, various safeguards are used. In the case of software, copy protection schemes which limit the number of copies that can be made or which corrupt the output when copying is detected have been employed. Another scheme causes software to become disabled after a predetermined period of time has lapsed.”); *id.* at 2:12-15 (“Yet another scheme is to distribute software, but which requires a ‘key’ to enable its use. This is employed in distribution schemes where ‘demos’ of the software are provided on a medium along with the entire product.”); *id.* at 2:51-3:3 (explaining that, “The [prior art] VPR system is self-contained and is comprised of : (1) point of sale kiosks for storing and downloading books; (2) personal storage mediums (cartridges) to which the books are downloaded, and (3) readers for viewing the book. . . . [T]he kiosk manages the number of ‘copies’ that may be checked out at any one time. Further, the copy of the book is erased from the user’s cartridge after a certain check-out time has expired.”); 3:47-50 (noting that in the Wave Systems prior art, “The system is installed onto a computer and collects information on what software is in use, encrypts it and then transmits the information to a transaction center.”);

- (b) none of the integrities require new or specially created hardware—the patents and inventors admit that the claims can be practiced using standard processors, regular communications channels (such as the Internet), and basic programming instructions, (*see, e.g.*, Dkt 459 at 84 (identifying corresponding structure for “means for processing a request” as “a general-purpose computer; and equivalents thereof”); Ex. 5 at 7:50-55 (“Examples of a rendering system may be a computer system, a digital audio system, or a printer.”); *id.* at 13:20-24,

29-31 (required hardware has only generic computer components: “a repository is comprised of a processing means 1200, storage system 1207, clock 1205 and external interface 1206.”); *id.* at 14:33-36 (“simple and inexpensive handheld repositories and network-based workstations may be suitable repositories, even though the measures and guarantees of security are modest”)); and

- (c) the three integrities were well-understood to be practiced together, as evidenced by the patents’ own description of the prior art Griswold, VPR, Sprague, Shear and other usage rights enforcement systems, (Ex. 4 at 1:62-3:54), each of which is described as having physical, communications and behavioral integrity, and by certain references cited on the face of the patent, *e.g.*, Tygar & Yee, (Ex. 20 at 124, 131, 145 (discussing physical integrity, *i.e.*, “physical shield” of hardware; communications integrity, *i.e.*, encryption; and behavioral integrity, *i.e.*, requirement of digital certificates).)

In short, “[t]he challenged claims also fail the second step of the *Alice* framework because they contain no meaningful limitations preventing the patentee from obtaining a monopoly over the abstract idea itself.” *Altec*, Slip Op. at 9; *see also Certusview*, 2015 WL 269427, at *20 (that claim elements (or combination) may be novel is not enough to constitute inventive concept).⁴

ContentGuard’s Opposition suggests that the “inventiveness” of the patent claims “is underscored by the PTAB’s recent decisions concerning the validity of four of these patents,” (Opp. at 15-16), and “by the numerous ‘objective indicia of non-obviousness’ that exist here,” (*id.* at 16). But this Court (and others) has squarely rejected the notion that prior proceedings *in which Section 101 issues were not considered* can shed any light on the patentable subject matter

⁴ ContentGuard suggests that “Defendants appear to have expressly abandoned all of their preemption arguments.” (Opp. at 13.) This is incorrect. Defendants simply did not present their preemption arguments in the Motion because, as the Supreme Court articulated in *Alice*, the focus of the second step of the *Mayo* test is whether the claims “‘disproportionately [ie] up the use of the underlying’ ideas.” 134 S.Ct. at 2354. It is now established that:

A patent need not . . . preempt an entire field to run afoul of § 101. Although courts have framed the “second-step” analysis in terms of preemption, there is no rule that ideas that do not preempt an entire field are *per se* patent eligible. Rather, the test as articulated by *Alice* is that there must be an inventive contribution on top of the underlying abstract idea.

Intellectual Ventures I LLC v. Symantec Corp., __F. Supp. 3d__, 2015 WL 1869690 at *17 (D. Del. Apr. 22, 2015) (quoting *Gametec LLC v. Zynga, Inc.*, 2014 WL 1665090, at *5 (N.D. Cal. Apr. 25, 2014) and *Money Suite*, 2015 WL 436160, at *5). As noted in Defendants’ Motion and this Reply, the Stefik patents’ extremely broad claims “disproportionately” tie up the underlying idea of enforcing usage rights and restrictions on digital content.

issue. As this Court explained when rejecting an argument virtually identical to ContentGuard's:

[Plaintiff] contends that the validity of the . . . Patent was tested and upheld in prior litigation. . . . [Plaintiff] argues that if the claim "preempted the abstract idea of preparing a sales proposal for a customer as alleged by [Defendant], it certainly would have been found anticipated or obvious in the [prior] case over the prior art that addressed the same fundamental concept." [Plaintiff] relies too much on the patents' prior history before this Court; the patent eligibility of these claims *under* § 101 is an issue of first impression. Although "the § 101 patent-eligibility inquiry and, say, the § 102 novelty inquiry might sometimes overlap," *Mayo*, 132 S. Ct. at 1304, the fact that the claim previously passed novelty and nonobviousness hurdles does not necessarily preclude invalidation under § 101.

Altec, Slip Op. at 11 (citing *Ultramercial*, 772 F.3d at 716; *see also Diamond*, 450 U.S. at 190 (§ 101 inquiry is distinct from other conditions of patentability)).

Finally, ContentGuard's Opposition argues that Defendants "have not demonstrated that the patents are devoid of inventiveness 'as an ordered combination'" (Opp. at 17.) In so arguing, ContentGuard ignores the multiple discussions in Defendants' Motion (*e.g.*, on pages 15, 17, 19 and 21) explaining how the claims follow the same "ordered combination" as a traditional library transaction: a library sets rules for the use of its materials, a patron makes a request to check out a book, a librarian verifies that the patron is trusted (*i.e.*, has a valid library card), the librarian provides access to the requested book to the trusted patron, and the patron uses the book in accord with the library's rules. In fact, as pointed out in Defendants' Motion, the Stefik specifications themselves recognize that this same basic ordering of steps was practiced by users of the prior art VPR Systems book "kiosks":

In a purchase transaction, a purchaser will purchase a voucher card representing the desired book. The voucher will contain sufficient information to identify the book purchased and perhaps some demographic information relating to the sales transaction. To download the book, the voucher and the cartridge are inserted into the kiosk.

The VPR system may also be used as a library. In such an embodiment, the kiosk manages the number of "copies" that may be checked out at one time. Further the copy of the book is erased from the user's cartridge after a certain check-out time has expired. However, individuals cannot loan books because the cartridges may only be used with the owner's reader.

(Ex. 4 at 2:57-3:1.) ContentGuard offers no explanation whatsoever for its bare assertion that the claims possess inventiveness as an ordered combination, (Opp. at 17), because, simply put, there

is nothing at all different or unique about the ordering of actions/elements in the Stefik patent claims. *See Open Text S.A. v. Box, Inc.*, No. 13-4910, 2015 WL 269036, at *5 (N.D. Cal. Jan. 20, 2015) (conclusory claim that ordered combination of elements is inventive insufficient).⁵

II. The Nguyen Patents

A. The Nguyen Patents Are Drawn to Abstract Ideas.

Defendants' Motion carefully explains and establishes, on a claim-by-claim basis, how the Nguyen patents are directed to the abstract idea of enforcing sublicensing rights and restrictions (which the patents name "meta-rights") on digital content. (Mot. at 28-37.) Once again, rather than engage in the proper and required claim-by-claim analysis, ContentGuard's Opposition lumps together the asserted Nguyen patent claims and simply makes the conclusory assertion that "These patents teach much more than an 'idea' that has existed in 'over-the-counter' commerce for quite some time" because "meta-rights" are "*enforceable by a repository*", rather than merely written agreements. (Opp. at 17-18.) This assertion misses the entire point of the patentable subject-matter analysis. It is now black-letter law that a claim does not qualify as patentable simply because it takes an old and abstract idea (*e.g.*, sublicensing) and specifies that the idea be performed on or by a computer. As stated by the Supreme Court in *Alice*, "Given the ubiquity of computers, wholly generic computer implementation is not generally the sort of 'additional feature' that provides any 'practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself.'" *Alice*, 134 S. Ct. at 2358 (quoting *Mayo*, 132 S. Ct at 1297); *see also Altec*, Slip Op. at 8.

As set forth in the claim charts and analysis in Defendants' Motion, (Mot. at 28-37), a "meta-right"—*i.e.*, "a right that, when exercised, creates or disposes of usage rights (or other meta-rights) but that is not itself a usage right . . .", (Dkt. 459 at 106)—is found, *e.g.*, in ordinary

⁵ ContentGuard suggests that "the subject matter of the Trusted Repository Patents is narrow, *i.e.*, limited to devices that maintain physical, communications, and behavioral integrity, rather than all devices that are capable to receive content via the Internet." (Opp. at 13). Yet, this suggestion is inconsistent with ContentGuard's own infringement and damages allegations in this case, which (a) attempt to use the doctrine of equivalents to expand the reach of the claims to cover virtually any and all digital rights management systems— not just "trusted" systems with the three integrities defined by the Court; and (b) assert that the Stefik patents are "essential" to the implementation of *any* commercially acceptable digital rights management system.

video rental transactions where movie studios give video stores (and/or a video store chain) the “meta-rights” to rent a certain movie titles to customers under prescribed terms and conditions. The mere facts that the asserted Nguyen patent claims (a) attempt to coin the term “meta-rights”, and (b) may generally require “meta-rights” to be provided in computer-enforceable form does not convert the abstract idea of sublicensing into a non-abstract invention eligible for patenting.⁶ The Court’s constructions and the Nguyen patent specifications “identify no inventive algorithms or otherwise creative means for [implementing the abstract idea] other than an instruction that the basic process be performed using generic computer components.” *Altec*, Slip Op. at 10.⁷

ContentGuard last argues that the Nguyen patent claims “specifically disclose and claim ‘state variable’ elements that are used to track and control the exercise of created rights, further removing these patents from the realm of patent-ineligible ideas.” (Opp. at 18.) This wholly unsupported and unexplained assertion is insufficient to save the Nguyen patent claims under Section 101. As detailed in the claim charts and the detailed explanations in Defendants’ Motion, the “state variable” element is found in basic human loan transactions, including, e.g., a video store rental transaction where a clerk keeps a paper or digital transaction log in which he records and tracks (a) the number of copies of a particular movie that are checked out of, and remain in, the store, (b) the time remaining on an individual customer’s movie rentals, and (c) the number of DVDs rented by a customer at a single time (which may be subject to limits

⁶ ContentGuard argues Defendants’ Motion is somehow affected by a statement from Apple’s counsel at the claim construction hearing to the effect that a meta-right is “not something that is abstract or generalized but it is used by a repository.” (Opp. at 18.) Apple counsel’s use of the word “abstract” in the *Markman* hearing to refer to the proper construction of “meta-right” obviously was not referencing the “abstract idea” concept of Section 101 and cannot be taken as any kind of admission that the construed term “meta-right” either escapes from or passes an appropriate Section 101 inquiry. As recognized by this Court in *Altec*, the mere fact that claim terms may refer to or include computer elements does not automatically confer patentability; generic and/or conventional computer implementation of an “abstract idea” is not patentable regardless of the amount of techno-speak used. *See Altec*, Slip Op. at 8-9.

⁷ As explained for the Stefik patents and illustrated in the Defendants’ hypotheticals, the Nguyen patent claims’ reference to “repositories” does not render the claims non-abstract, as (a) the three integrities required of “repositories” are similarly maintained by movie studios, movie stores, store clerks and customers in video store rental transactions (just as they are in similar library loan transactions), (b) the Nguyen patents, like the Stefik patents, require no specific or defined hardware and no specific or complex programming for a computing element to qualify as a “repository”, and (c) the computer elements, functions and technique usable to maintain the three integrities are basic and conventional—secure storage, basic encryption/decryption and processing of data, and faithful execution of software instructions. *See supra* at 5-7, 10-11; *see also* Mot. at 9-16.

established by the store). That the Nguyen claims specify that “state variables” are automatically tracked by a computer, rather than being tracked by a human store clerk using pen-and-paper or a computer, does not entitle ContentGuard to a 20-year monopoly on the idea of computer-enforced sublicensing. *Altec*, Slip Op. at 9.⁸

Though ContentGuard cites a California case to argue that the video store hypothetical is “unhelpful for computer inventions” because a human cannot efficiently write “the 1s and 0s comprising a computer program and applying the same algorithms”, (Opp. at 18), binding authority is clear that such hypothetical analysis and comparison is exactly the type that should be used to test the patentability of purported computer inventions. *See Content Extraction*, 776 F.3d at 1347 (rejecting argument that claim was not abstract “because human minds cannot process and recognize the stream of bits” involved in the computer implementation, and applying hypothetical of human performance); *Altec*, Slip Op. at 7 (“The steps performed by the claimed computer elements are functional in nature and could easily be performed by a human.”).

B. The Nguyen Patents Have No Inventive Concept.

The Nguyen patents claim only generic computer functionality: “the invention can be implemented through any type of devices [sic], such as computers and computer systems . . . the various functions can be accomplished in any manner through hardware and/or software. . . . Devices can include personal computers, workstations, thin clients, PDAs and the like.” (*See, e.g.*, Ex. 11 at 14:50-51, 58-59, 65-67.) ContentGuard asserts that the inventive element is in the combination of “among other [unspecified] things,” meta-rights, repositories, and state variables, although once again ContentGuard neglects to explain how this combination of generic computer functionalities could possibly constitute an inventive element. Such a conclusory assertion fails to establish an inventive element. *Open Text*, 2015 WL 269036, at *5.

Simply put, the Nguyen patents do not, and cannot, claim a patentable invention simply by specifying that the idea of sublicensing rights to digital content be performed by secure and reliable computers, rather than fallible humans.

⁸ The Nguyen patents make clear that only generic and conventional computer functionality is required to implement the “state variable” element. (Ex. 11 at 13:54 (“A counter is a common form of state variable usage.”).)

CONCLUSION

For the forgoing reasons, as well as those discussed in the Motion, Defendants respectfully request that their Motion for Judgment on the Pleadings be granted.

Respectfully submitted,

Dated: May 18, 2015

By: /s/ Robert Unikel

Robert W. Unikel (admitted *pro hac vice*)
KAYE SCHOLER LLP
70 W. Madison St., Suite 4200
Chicago, IL 60602-4231
Telephone: (312) 583-2300
Facsimile: (312) 583-2360
Email: robert.unikel@kayescholer.com

J. Mark Mann
State Bar No. 12926150
Gregory Bake Thompson
State Bar No. 24242033
MANN TINDEL & THOMPSON
300 W. Main
Henderson, TX 75652
Telephone: (903) 657-8540
Facsimile: (903) 657-6003
Email: mark@themannfirm.com
blake@themannfirm.com

Michael J. Malecek
Timothy K. Chao (admitted *pro hac vice*)
KAYE SCHOLER LLP
3000 El Camino Real
2 Palo Alto Square, Suite 400
Palo Alto, CA 94306
Telephone: (650) 319-4500
Facsimile: (650) 319-4700
Email: michael.malecek@kayescholer.com
timothy.chao@kayescholer.com

Attorneys for Motorola Mobility, LLC

/s/ Jennifer Haltom Doan

Glen E. Summers (admitted pro hac vice)
glen.summers@bartlit-beck.com
Alison G. Wheeler (admitted pro hac vice)
alison.wheeler@bartlit-beck.com
Katherine Hacker (admitted pro hac vice)
kat.hacker@bartlit-beck.com
BARTLIT BECK HERMAN PALENCHAR &
SCOTT LLP
1899 Wynkoop Street, 8th Floor
Denver, CO 80202
Telephone: (303) 592-3100
Facsimile: (303) 592-3140:

Counsel for Defendant AMAZON.COM, INC.

Jennifer Haltom Doan
Texas State Bar No. 08809050
jdoan@haltomdoan.com
Joshua Reed Thane
Texas Bar No. 24060713
jthane@haltomdoan.com
HALTOM & DOAN
6500 Summerhill Road
Crown Executive Center, Suite 100
Texarkana, TX 75505
Telephone: (903) 255-1000
Facsimile: (903) 255-0800

Counsel for Defendant AMAZON.COM, INC.

Michael Valaik (admitted pro hac vie)
michael.valaik@bartlit-beck.com
Abby Mollen (admitted pro hac vice)
abby.mollen@bartlit-beck.com
Joshua Ackerman (admitted pro hac vice)
joshua.ackerman@bartlit-beck.com
BARTLIT BECK HERMAN PALENCHAR &
SCOTT LLP
54 West Hubbard Street, #300
Chicago, IL 60654
Telephone: (312) 494-4400
Facsimile: (312) 494-4440

Counsel for Defendant AMAZON.COM, INC.

/s/ Melissa Richards Smith

Bryan K. Anderson
Bkanderson@sidley.com
Nathan Greenblatt
Ngreenblatt@sidley.com
SIDLEY AUSTIN LLP
1001 Page Mill Road, Building 1
Palo Alto, CA 94304
Telephone: (650) 565-7007
Facsimile: (650) 565-7100

Counsel for Defendant APPLE INC.

Melissa Richards Smith
Texas State Bar No. 24001351
Melissa@gillamsmithlaw.com
GILLAM & SMITH LLP
303 South Washington Avenue
Marshall, TX 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

Counsel for Defendant APPLE INC.

David T. Pritikin
Dpritikin@sidley.com
Richard A. Cederroth
Rcederth@sidley.com
Nathaniel C. Love
Nlove@sidley.com
SIDLEY AUSTIN LLP
One South Dearborn Street
Chicago, IL 60603
Telephone: (312) 853-7000
Facsimile: (312) 853-7036

Counsel for Defendant APPLE INC.

/s/ Scott Partridge
Scott Partridge
Texas Bar No. 00786940
Scott.partridge@bakerbotts.com
Lisa Kelly
Texas State Bar No. 24041659
Lisa.kelly@bakerbotts.com
Bradley Bowling
Texas State Bar No. 24040555
Brad.bowling@bakerbotts.com
Baker Botts LLP
One Shell Plaza
901 Louisiana
Houston, TX 77002
Telephone: 713-229-1569
Facsimile: 713-229-7769

Counsel for Defendant HUAWEI
TECHNOLOGIES CO., LTD. and HUAWEI
DEVICE USA, INC.

Peter J. Wied
Pwied@goodwinprocter.com
Vincent K. Yip
Vyip@goodwinprocter.com
Jay Chiu
Jchiu@goodwinprocter.com
Goodwin Procter LLP
601 S. Figueroa Street, 41st Floor
Los Angeles, CA 90017
Telephone: 213-426-2500

/s/ Eric H. Findlay
Eric H. Findlay
Efindlay@findlaycraft.com
Brian Craft
Bcraft@findlaycraft.com
Findlay Craft, P.C.
102 N. College Avenue, Suite 900
Tyler, TX 75702
Telephone: 903-534-1100
Facsimile: 903-534-1137

Facsimile: 213-623-1673

Counsel for Defendants HTC CORP. and HTC
AMERICA, INC.

Counsel for Defendants HTC CORP. and HTC
AMERICA, INC.

/s/ Michael Joseph Barta

Neil Phillip Sirota
Neil.sirota@bakerbotts.com
Robert Lawrence Maier
Robert.maier@bakerbotts.com
Brian Boerman
Brian.boerman@bakerbotts.com
Guy Eddon
Guy.eddon@bakerbotts.com
Baker Botts LLP
30 Rockefeller Plaza, 44th Floor
New York, NY 10112
Telephone: (212) 408-2548
Facsimile: (212) 259-2548

Counsel for Defendants SAMSUNG
ELECTRONICS CO., LTD. SAMSUNG
ELECTRONICS AMERICA, INC. and
SAMSUNG TELECOMMUNICATIONS
AMERICA, LLC

Michael E. Jones
Texas State Bar No.10929400
Mikejones@potterminton.com
Allen F. Gardner
Texas State Bar No.24043679
Allengardner@potterminton.com
Potter Minton, A Professional Corporation
110 North College, Suite 500
Tyler, TX 75702
Telephone: 903-597-8311
Facsimile: 903-593-0846

Counsel for Defendants SAMSUNG
ELECTRONICS CO., LTD. SAMSUNG
ELECTRONICS AMERICA, INC. and
SAMSUNG TELECOMMUNICATIONS
AMERICA, LLC

Michael Joseph Barta
Michael.barta@bakerbotts.com
Baker Botts LLP
The Warner
1299 Pennsylvania Avenue NW
Washington, DC 20004
Telephone: (202) 639-7703
Facsimile: (202) 585-1058

Counsel for Defendants SAMSUNG
ELECTRONICS CO., LTD. SAMSUNG
ELECTRONICS AMERICA, INC. and
SAMSUNG TELECOMMUNICATIONS
AMERICA, LLC

CERTIFICATE OF SERVICE

I hereby certify that counsel of record who are deemed to have consented to electronic service are being served this 18th day of May, 2015, with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3).

By /s/ Robert Unikel